

Windows-агент инициализации для подключения сканера WinRS

В данной статье описана конфигурация Windows-агента инициализации для подключения сканера WinRS к клиентскому устройству, а также приведена пользовательская инструкция по использованию агента инициализации.

Конфигурация агента инициализации

Для автоматической предварительной конфигурации конечных устройств, которые будут сканироваться перед подключением к сети, вы можете использовать агент инициализации. Чтобы реализовать данный функционал, выполните следующие действия:

Шаг 1. Выполните конфигурацию сканера WinRS. Для этого перейдите в раздел **Конфигурация → Соответствие → Механизмы сканирования** и создайте новый механизм сканирования с типом WinRS. Подробное описание процесса конфигурации сканера приведено в статье [Конфигурация сканеров соответствия в AxelNAC](#).

Шаг 2. Настройте интеграцию AxelNAC с PKI-провайдером. Для этого перейдите в раздел **Конфигурация → Расширенные настройки доступа → PKI-провайдеры**, нажмите **Новый PKI-провайдер** и в выпадающем списке выберите значение **SCEP** для интеграции с Microsoft PKI или **AxelNAC PKI** для интеграции с встроенным PKI-провайдером AxelNAC. Подробное описание процесса интеграции с PKI-провайдерами описано в разделе [Интеграция PKI](#).

Шаг 3. Для создания нового агента инициализации перейдите в раздел **Конфигурация → Расширенные настройки доступа → Агенты инициализации**, нажмите **Новый агент инициализации** и в выпадающем списке выберите значение **Windows**.

Шаг 4. В открывшемся окне выполните конфигурацию агента инициализации:

- **ID инициализации** — название агента инициализации, которое отображается в списке агентов;
- **Описание** — описание агента инициализации, которое отображается в списке агентов;
- **Обеспечить выполнение** — данный параметр определяет, необходимо ли принудительное использование агента инициализации при порտальной или RADIUS-аутентификации;
- **Авторегистрация** — данный параметр определяет, регистрировать ли устройства в сети автоматически, если они авторизованы в агенте инициализации;
- **Применить роль** — при активации данного параметра, указанная ниже роль будет применяться к конечному устройству, если оно авторизовано в агенте инициализации;
- **Применяемые роли** — список ролей, которые будут применяться при авторизации устройства;
- **Роли** — список ролей, для которых будет использоваться агент инициализации;
- **SSID** — идентификатор беспроводной сети, для которой будет использоваться агент инициализации;
- **Широковещательная сеть** — данный параметр определяет, является ли указанная сеть скрытой;
- **Тип безопасности** — тип защиты, применяемый в указанной беспроводной сети. Может принимать значения **Открытые, WEP, WPA и WPA2**;
- **Тип EAP** — применяемый метод EAP. Данный параметр может принимать следующие значения:
 - **PEAP** — при выборе данного метода будут доступны следующие поля:
 - **Файл сертификата сервера RADIUS** — поле для загрузки сертификата RADIUS-сервера;
 - **Файл CA сервера RADIUS** — поле для загрузки сертификата центра сертификации.
 - **EAP-TLS** — при выборе данного метода будут доступны следующие поля:
 - **PKI-провайдер** — поле для выбора предварительно настроенного PKI-провайдера, которые будет работать совместно с агентом инициализации.
 - **No EAP** — при выборе данного метода будут доступны следующие поля:
 - **Включить DPSK** — при активации данного параметра, для каждого нового соединения будет генерироваться новый PSK-ключ;
 - **Использовать локальный пароль для DPSK повторно** — при активации данного параметра, для пользователей, которые уже авторизовывались через данный агент инициализации, будет использоваться PSK-ключ, созданный при первой авторизации;
 - **Ключ Wi-Fi** — пароль для подключения к беспроводной сети.
- **Сканер WinRS** — поле для выбора предварительно настроенного механизма сканирования, для которого агент инициализации создаст учетную запись (в данном поле будут доступны механизмы сканирования, у которых в качестве метода аутентификации выбрано значение **По сертификату** или **Базовый через HTTPS**).

Для сохранения агента нажмите **Создать**.

Шаг 5. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Профили подключения** и выберите открытый профиль подключения, который будет использоваться для распространения агента инициализации. В окне конфигурации профиля подключения, в поле **Агенты инициализации** выберите агент, который вы создали в шаге 4 и нажмите **Сохранить**.

Шаг 6. Выберите закрытый профиль подключения, который используется для доступа к внутренней сети. В окне конфигурации профиля подключения, в поле **Сканеры** выберите механизм сканирования, для которого был сконфигурирован агент инициализации и нажмите **Сохранить**.

SSID закрытой сети в профиле подключения должен совпадать с SSID, указанным в агенте инициализации.

Теперь, при подключении к сети, пользователю будет предложено указать электронную почту и пароль, для которых будет сгенерирован сертификат. После указания учетных данных, появится ссылка для скачивания агента инициализации, который произведет конфигурацию конечного устройства для работы со сканером соответствия.

Подключение к сети с помощью агента инициализации

Вы можете [скачать](#) и использовать данную инструкцию для взаимодействия с вашими пользователями.

В нашей сети используется механизм сканирования, который проверяет ваше устройство на соответствие требованиям и политикам ИБ. Для того, чтобы сканер мог авторизоваться на вашем устройстве, необходимо произвести первичную конфигурацию вашего АРМ.

Первое подключение к сети

При первом подключении к сети, вы будете перенаправлены на Captive-портал. Внимательно прочтите условия использования доступа к сети и примите их. Укажите свою электронную почту, которая будет использоваться для генерации сертификата. Пароль генерируется автоматически, но вы можете указать свой собственный. Нажмите **Сгенерировать сертификат**.

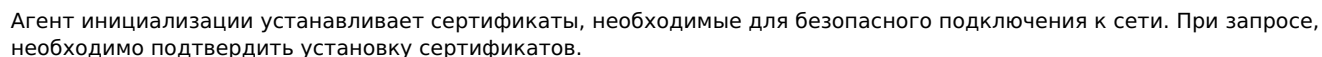
The screenshot shows the AxelNAS Captive Portal interface. At the top is the AxelNAS logo. Below it, the text reads "Генерация сертификата для подключения EAP TLS". A second line of text repeats "Генерация сертификата для подключения EAP TLS". A paragraph explains that to complete registration, a user certificate must be generated, and a random password is provided. Below this, it says "Ниже можно также изменить пароль." and shows two input fields: "ЭЛЕКТРОННАЯ ПОЧТА" (empty) and "ПАРОЛЬ" (containing "leregry"). A button labeled "Сгенерировать сертификат" is below the password field. At the bottom, there is a footer with support information and device details: "IP 10.31.205.209" and "MAC 90:de:80:8a:77:94".

После генерации сертификата вам будет предложено установить агент инициализации, который произведет конфигурацию вашего устройства. Для установки агента нажмите **Установить агент**.

The screenshot shows the AxelNAS Captive Portal interface for agent installation. The AxelNAS logo is at the top. Below it, the text reads "Provisioning : provisn_test". A paragraph explains that to complete connection to a secure SSID, the user must launch the agent. Below this, there is a large red button labeled "Установить агент". A blue arrow points from the text "предлагаемый ниже агент" to the button. Below the button is a blue link labeled "Продолжить". At the bottom, there is a footer with support information and device details: "IP 10.31.205.209" and "MAC 90:de:80:8a:77:94".

После нажатия, будет скачан исполняемый файл. По завершении загрузки, запустите его.

В открывшемся окне нажмите **Настройка соединения** Вам будет предложено ввести пароль, который указывался при генерации сертификата. Введите пароль и нажмите **ОК**. После этого, ваше устройство будет автоматически сконфигурировано для работы с механизмом сканирования.



ID стат'и: 350

Последнее обновление: 30 окт., 2024

Обновлено от: Егоров В.

Ревизия: 7

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.2.0 -> AxelNAC. Руководство администратора -> Интеграция с агентами инициализации -> Windows-агент инициализации для подключения сканера WinRS

<https://docs.axel.pro/entry/350/>